

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-218875

(43)Date of publication of application : 31.07.2003

(51)Int.Cl. H04L 12/28  
 H04B 1/06  
 H04L 9/08  
 H04Q 7/38

(21)Application number : 2002-009596

(71)Applicant : SEIKO EPSON CORP

(22)Date of filing : 18.01.2002

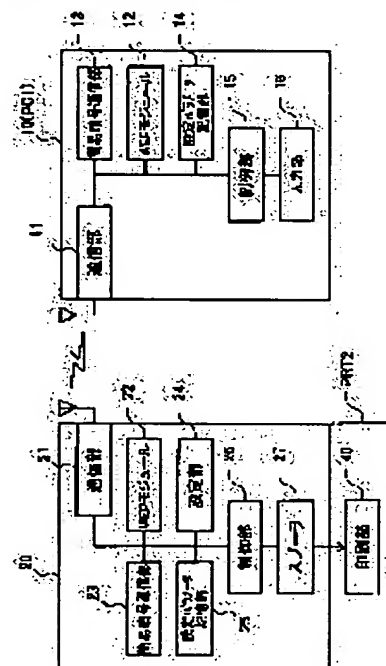
(72)Inventor : SHIOBARA SUSUMU  
 GASSHO KAZUTO

## (54) SETTING OF PARAMETER FOR RADIO COMMUNICATION APPARATUS

## (57)Abstract:

PROBLEM TO BE SOLVED: To avoid leakage of setting parameters when setting to a new radio communication apparatus by the communication apparatus.

SOLUTION: On a side of a radio communication apparatus 10, the setting parameters for establishing connections to existing radio LAN are encrypted in an easy manner and transmitted to a radio print server 20. On a side of the print server 20, the simply encrypted setting parameters transmitted from the communication apparatus 10 are received and decrypted to be set. A simple encryption method and a simple decryption method are previously known between the communication apparatus 10 and the print server 20.



## LEGAL STATUS

[Date of request for examination]

25.06.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's]

decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-218875

(P2003-218875A)

(43)公開日 平成15年7月31日(2003.7.31)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テマコード*(参考)
H 0 4 L 12/28	2 0 0	H 0 4 L 12/28	2 0 0 Z 5 J 1 0 4
H 0 4 B 1/06		H 0 4 B 1/06	Z 5 K 0 3 3
H 0 4 L 9/08		7/26	1 0 9 R 5 K 0 6 1
H 0 4 Q 7/38		H 0 4 L 9/00	6 0 1 C 5 K 0 6 7

審査請求 未請求 請求項の数10 O L (全 9 頁)

(21)出願番号 特願2002-9596(P2002-9596)

(22)出願日 平成14年1月18日(2002.1.18)

(71)出願人 000002369

セイコーエプソン株式会社

東京都新宿区西新宿2丁目4番1号

(72)発明者 塩原 進

長野県諏訪市大和三丁目3番5号 セイコーエプソン株式会社内

(72)発明者 合掌 和人

長野県諏訪市大和三丁目3番5号 セイコーエプソン株式会社内

(74)代理人 110000028

特許業務法人明成国際特許事務所

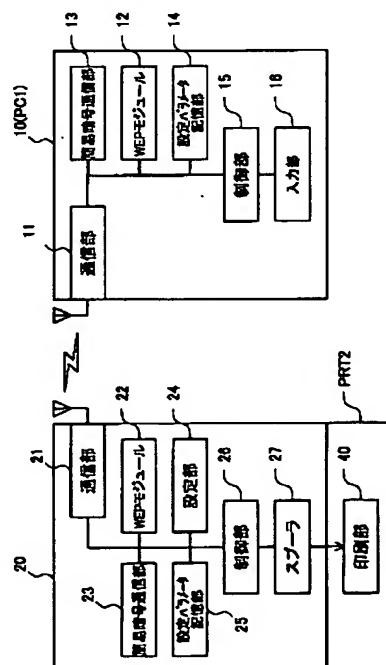
最終頁に続く

(54)【発明の名称】 無線通信装置へのパラメータの設定

(57)【要約】

【課題】 無線通信装置によって新たな無線通信装置の設定を行う際に、設定パラメータの漏洩を回避する。

【解決手段】 無線通信装置10側で、既存の無線LANへの接続を確立するための設定パラメータを簡易暗号化し、無線プリントサーバ20に送信する。無線プリントサーバ20側では、無線通信装置10から送信された簡易暗号化された設定パラメータを受信して復号し、設定する。なお、簡易暗号化および簡易復号の方法は、無線通信装置10と無線プリントサーバ20との間で予め既知である。



## 【特許請求の範囲】

【請求項 1】 無線通信装置であって、無線通信に用いられる設定パラメータを記憶する設定パラメータ記憶部と、前記設定パラメータの送信先となる他の無線通信装置との間で、前記設定パラメータの送信用に予め用意された方法で、該設定パラメータを暗号化する暗号化部と、該暗号化された設定パラメータを前記他の無線通信装置に送信する送信部と、を備える無線通信装置。

【請求項 2】 請求項 1 記載の無線通信装置であって、前記設定パラメータは、暗号化通信を確立するための鍵情報を含む、無線通信装置。

【請求項 3】 請求項 1 記載の無線通信装置であって、更に、前記他の無線通信装置に設定されており、暗号化通信を確立するための鍵情報を入力する鍵入力部を備え、前記暗号化部は、前記鍵情報を用いて前記暗号化を行う、無線通信装置。

【請求項 4】 無線通信装置であって、請求項 1 記載の無線通信装置側で暗号化された設定パラメータを受信する受信部と、該受信した設定パラメータを、前記暗号化に対応した既知の方法で復号する復号部と、該復号された設定パラメータに基づいて、前記無線通信の設定を行う設定部と、を備える無線通信装置。

【請求項 5】 請求項 4 記載の無線通信装置であって、更に、前記復号部で用いられ、暗号化通信を確立するための鍵情報を乱数的に生成する鍵情報生成部と、該生成された鍵情報を可視的に出力する出力部と、を備える無線通信装置。

【請求項 6】 請求項 4 記載の無線通信装置であって、前記復号部で用いられ、暗号化通信を確立するための鍵情報は、予め設定された情報である、無線通信装置。

【請求項 7】 請求項 4 記載の無線通信装置を備えるプリントサーバ。

【請求項 8】 無線通信装置を用いて、他の無線通信装置に対し、無線通信に用いられる設定パラメータを設定する設定方法であって、(a) 前記設定パラメータを取得する工程と、(b) 前記他の無線通信装置との間で、前記設定パラメータの送信用に予め用意された方法で、前記設定パラメータを暗号化する工程と、(c) 該暗号化された設定パラメータを前記他の無線通信装置に送信する工程と、を備える設定方法。

【請求項 9】 無線通信装置を用いて、他の無線通信装

置に対し、無線通信に用いられる設定パラメータを設定するためのコンピュータプログラムであって、前記設定パラメータを取得する機能と、前記他の無線通信装置との間で、前記設定パラメータの送信用に予め用意された方法で、前記設定パラメータを暗号化する機能と、該暗号化された設定パラメータを前記他の無線通信装置に送信する機能と、をコンピュータに実現させるためのコンピュータプログラム。

【請求項 10】 請求項 9 記載のコンピュータプログラムをコンピュータ読み取り可能に記録した記録媒体。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、無線通信装置へのパラメータの設定に関する。

【0002】

【従来の技術】従来、複数のコンピュータやプリンタ等の周辺機器を接続した LAN (Local Area Network) が普及している。近年では、接続にケーブルを用いない無線 LAN が普及しつつある。無線 LAN では、一般に、電波を用いた無線通信を行う無線通信装置が用いられる。この無線 LAN では、装置間での通信を確立するために、各種パラメータの設定が必要である。更に、第三者へのデータの漏洩を防止するために、暗号化通信が行われる場合もある。暗号化通信では、暗号化用あるいは復号用の鍵情報を各無線通信装置に設定しておく必要がある。既に構築されている無線 LAN に新たな無線通信装置を接続する場合、これらの設定は、一方の無線通信装置から他方の無線通信装置に、無線通信で鍵情報等の設定パラメータを送信することによって行われることがある。

【0003】

【発明が解決しようとする課題】しかし、設定時は、受信側無線通信装置にとって、暗号化通信を行うための鍵情報は未知であるので、設定パラメータの送受信は、必然的に非暗号化通信で行われていた。このため、設定パラメータが第三者に漏洩するおそれがあり、無線通信におけるセキュリティを確保することができないおそれがあった。

【0004】かかる課題は、無線プリントサーバなど、パラメータの入力を行うための十分なインタフェースを備えていない無線通信装置への設定時には、特に深刻であった。

【0005】本発明は、上述の課題を解決するためになされたものであり、無線通信装置によって新たな無線通信装置の設定を行う際に、設定パラメータの漏洩を回避することを目的とする。

【0006】

【課題を解決するための手段およびその作用・効果】上

述の課題の少なくとも一部を解決するため、本発明では、以下の構成を採用した。本発明の第1の無線通信装置は、無線通信装置であって、無線通信に用いられる設定パラメータを記憶する設定パラメータ記憶部と、前記設定パラメータの送信先となる他の無線通信装置との間で、前記設定パラメータの送信用に予め用意された方法で、該設定パラメータを暗号化する暗号化部と、該暗号化された設定パラメータを前記他の無線通信装置に送信する送信部と、を備えることを要旨とする。

【0007】本発明では、無線通信用の設定パラメータを、送信先となる他の無線通信装置との間で設定パラメータの設定用に予め用意された方法で暗号化して、他の無線通信装置に送信する。こうすることによって、暗号化および復号の方法を知らない第三者への設定パラメータの漏洩を回避することができる。従って、無線通信におけるセキュリティを確保しつつ、新たに設置される無線通信装置に、設定パラメータを、無線通信を介して設定することができる。

【0008】ここで、「設定パラメータ」とは、例えば、国際標準規格IEEE802.11に基づく無線通信におけるESS-ID、WEPキー、通信モード、通信チャンネルなどが含まれる。

【0009】また、「送信先となる他の無線通信装置との間で、前記設定パラメータの送信用に予め用意された方法」とは、例えば、データの配列を2ビットずつずらすなど、予め決められた固有の規則に従って単にデータにスクランブル化をかける方法や、送信側と受信側との双方で既知の秘密鍵（共通鍵ともいう）を用いる方法などが挙げられる。

【0010】なお、本発明は、Bluetooth（商標）やHomeRF（商標）等の規格に基づいた電波を用いた無線通信装置や、光や音などを用いた無線通信装置にも適用可能である。

【0011】本発明の第1の無線通信装置において、前記設定パラメータは、暗号化通信を確立するための鍵情報を含むようにすることが好ましい。

【0012】こうすることによって、鍵情報の漏洩を回避でき、無線通信のセキュリティを向上させることができる。ここで、「鍵情報」とは、データの暗号化および復号に用いられる鍵に関する情報を意味している。鍵情報としては、例えば、国際標準規格IEEE802.11で採用されているWEP（Wired Equivalent Privacy）と呼ばれる暗号技術で用いられるWEPキー（共通鍵）が挙げられる。鍵情報には、また、先に例示した他の規格に基づいた無線通信に用いられる鍵に関する情報も含まれ得る。

【0013】本発明の第1の無線通信装置において、更に、前記他の無線通信装置に設定されており、暗号化通信を確立するための鍵情報を入力する鍵入力部を備え、前記暗号化部は、前記鍵情報を用いて前記暗号化を行う

ようにしてもよい。

【0014】このように、受信装置側で設定されている鍵情報を、送信側に入力することにより、設定パラメータの送信に鍵情報を用いた暗号化を施すことができるため、単なる規則的なスクランブルをかける方法よりもセキュリティを向上させることができる。受信装置側に設定されている鍵情報は、例えば、予めマニュアル等に記載しておくものとしてもよいし、受信装置側に設けられた表示パネル等に表示させるものとしてもよい。

【0015】本発明は、上述した本発明の第1の無線通信装置から暗号化された設定パラメータを受信する無線通信装置の発明として構成することもできる。つまり、この無線通信装置は、上述した無線通信装置とサブコンピネーションの関係に相当する。

【0016】本発明の第2の無線通信装置は、無線通信装置であって、請求項1記載の無線通信装置側で暗号化された設定パラメータを受信する受信部と、該受信した設定パラメータを、前記暗号化に対応した既知の方法で復号する復号部と、該復号された設定パラメータに基づいて、前記無線通信の設定を行う設定部と、を備えることを要旨とする。

【0017】こうすることによって、無線通信を確立するための設定パラメータを、第三者に漏洩することなく、無線通信を介して受信側無線通信装置に設定することができる。

【0018】本発明の第2の無線通信装置において、更に、前記復号部で用いられ、暗号化通信を確立するための鍵情報を乱数的に生成する鍵情報生成部と、該生成された鍵情報を可視的に出力する出力部と、を備えるようにしてもよい。

【0019】「可視的に出力する」とは、受信装置側に設けられた表示パネル等に表示する方法や、受信側無線通信装置に接続された印刷装置によって印刷する方法など視覚に訴える出力態様を意味する。受信側無線通信装置で鍵情報を生成し、可視的に出力することによって、受信側無線通信装置と暗号化通信を確立するための鍵情報を送信側無線通信装置に知らせることができる。送信側無線通信装置側は、出力された鍵情報を用いた暗号化を行うことによって、暗号化通信を確立することができる。

【0020】なお、本発明の第2の無線通信装置において、前記復号部で用いられ、暗号化通信を確立するための鍵情報は、予め設定された情報であるものとしてもよい。

【0021】予め設定された鍵情報は、例えば、無線通信装置本体に表示されてもよいし、マニュアルに記載されていてもよい。この受信側無線通信装置側に予め設定された鍵情報を用いた暗号化を、送信側無線装置側で行うことによって、暗号化通信を確立することができる。

【0022】本発明は、無線通信を利用可能な種々の機

器に適用可能である。例えば、本発明の第2の無線通信装置を備えるプリントサーバとして構成することも可能である。

【0023】プリントサーバは、通常、十分な入力インタフェースを備えていない。従って、本発明のプリントサーバによって、セキュリティを確保しつつ、上述したパラメータの設定を容易に行うことができる。

【0024】本発明は、上述の無線通信装置としての構成の他、無線通信に用いられる設定パラメータの設定方法の発明として構成することもできる。また、これを実現するコンピュータプログラム、およびそのプログラムを記録した記録媒体、そのプログラムを含み搬送波内に具現化されたデータ信号など種々の態様で実現することが可能である。なお、それぞれの態様において、先に示した種々の付加的要素を適用することが可能である。

【0025】本発明をコンピュータプログラムまたはそのプログラムを記録した記録媒体等として構成する場合には、無線通信装置を駆動するプログラム全体として構成するものとしてもよいし、本発明の機能を果たす部分のみを構成するものとしてもよい。また、記録媒体としては、フレキシブルディスクやCD-ROM、光磁気ディスク、ICカード、ROMカートリッジ、パンチカード、バーコードなどの符号が印刷された印刷物、コンピュータの内部記憶装置（RAMやROMなどのメモリ）および外部記憶装置などコンピュータが読み取り可能な種々の媒体を利用できる。

【0026】

【発明の実施の形態】以下、本発明の実施の形態について、実施例に基づき以下の順で説明する。

A. 第1実施例：

A1. 無線LANの構成：

A2. 無線通信装置：

A3. パラメータ設定：

B. 第2実施例：

B1. 無線通信装置：

B2. パラメータ設定：

C. 変形例：

【0027】A. 第1実施例：

A1. 無線LANの構成：図1は、無線LAN100の構成を示す説明図である。本実施例では、国際標準規格IEEE802.11に基づく無線LANを例に説明する。この無線LAN100は、複数のパーソナルコンピュータPC1、PC2、PC3、PC4と、プリンタPRT1と、アクセスポイントAPとから構成されている。パーソナルコンピュータPC1、PC2、PC3、PC4は、それぞれCPU、RAM、ROMおよび無線LANカードを備えている。更に、パーソナルコンピュータPC1、PC2、PC3、PC4それぞれには、無線LANカード用のユーティリティソフトがインストールされている。パーソナルコンピュータPC1、PC

2、PC3、PC4は、それぞれ無線通信装置として機能する。プリンタPRT1には、無線通信装置を有する無線プリントサーバが接続されている。

【0028】無線LAN100では、アクセスポイントAPを経由して無線通信を行う通信モード（インフラストラクチャ・モード）で各機器間の無線通信を行っている。従って、各パーソナルコンピュータPC1、PC2、PC3、PC4、およびプリンタPRT1に接続された無線プリントサーバには、それぞれ無線LANの各ネットワークをグループ分けするための識別情報であるESS-IDや、暗号通信を確立するための鍵情報としてのWEPキーや、通信モード等の各種パラメータが設定されている。共通のパラメータが設定されている機器間でのみ無線暗号化通信が可能である。本実施例では、無線LAN100のESS-IDを「group」、WEPキーを「ABCD」とした。

【0029】ここで、既存の無線LAN100に、新たに無線プリントサーバ20を備えるプリンタPRT2を無線接続する。そのためには、無線プリントサーバ20に上述した各種パラメータを設定する必要がある。本実施例では、無線通信装置10としてのパーソナルコンピュータPC1から無線通信を介して無線プリントサーバ20にパラメータを設定する。このようにアクセスポイントAPを経由せずに、無線通信装置同士で無線通信を行う通信モードをアドホック・モードと呼ぶ。このアドホック・モードによる無線暗号化通信では、WEPキーの他に（アドホック・モードでは、ESS-IDは使用しない）、無線通信に用いられる電波の周波数を特定する通信チャンネルの設定が必要となる。無線プリントサーバ20には、通信チャンネルのデフォルト値として「14」が設定されているものとする。

【0030】A2. 無線通信装置：図2は、本発明の第1実施例としての無線通信装置10および無線プリントサーバ20の概略構成を示す説明図である。無線通信装置10は、通信部11と、WEPモジュール12と、簡易暗号通信部13と、設定パラメータ記憶部14と、制御部15と、入力部16とを備えている。これらの機能ブロックは、パーソナルコンピュータPC1にパラメータ設定用のユーティリティソフトをインストールすることにより、ソフトウェア的に構築されている。ハードウェア的に構築してもよい。

【0031】設定パラメータ記憶部14は、無線LAN100への接続を確立するための各種設定パラメータを記憶している（図1参照）。WEPモジュール12は、無線LAN100に接続されているときに、設定パラメータ記憶部14に記憶されているWEPキー「ABCD」を用いてデータの暗号化および復号を行う。簡易暗号通信部13は、無線プリントサーバ20と無線通信を行うときに、データを簡易的に暗号化（以下、簡易暗号化と呼ぶ）する。本実施例では、データの配列を2ビット

トずつずらすことによって簡易暗号化するものとした。なお、この簡易暗号化の方法は、無線プリントサーバ20との間で予め既知であるものとする。通信部11は、暗号化あるいは簡易暗号化されたデータをバケットに分割し、設定パラメータ記憶部14に記憶されている設定パラメータに基づいて、無線LANカードから送信する。つまり、通信部11は、無線LANカードを制御するデバイスドライバとしての機能を有している。入力部16は、キーボード、マウス等からの指示を入力する。上記各部は、制御部15によって制御される。

【0032】無線プリントサーバ20は、通信部21と、WEPモジュール22と、簡易暗号通信部23と、設定部24と、設定パラメータ記憶部25と、制御部26と、スプーラ27とを備えている。通信部21は、無線通信装置10から送信されたバケットを受信し、結合する。WEPモジュール22は、無線LAN100に接続されているときに、WEPキーを用いてデータの暗号化および復号を行う。簡易暗号通信部23は、無線通信装置10の簡易暗号通信部13に対応した簡易的な復号（以下、簡易復号と呼ぶ）を行う。本実施例では、データの配列を2ビットずつ簡易暗号通信部13と逆方向にずらすことによって、簡易復号を行う。設定パラメータ記憶部25は、無線通信用の設定パラメータを記憶しており、当初は、図1に示した通り、「ESS-ID:なし、WEPキー:なし」などの設定が記憶されている。設定部24は、設定パラメータ記憶部25の内容を、簡易復号された設定パラメータの内容に更新する。なお、設定パラメータ記憶部25には、デフォルト値の設定パラメータと、新規の設定された設定パラメータとが別々に記憶されるようにしてもよい。スプーラ27は、印刷ジョブの保持、管理、印刷部40への出力など、プリントサーバとしての主機能を実現する。

【0033】A3. パラメータ設定: 図3は、第1実施例における設定パラメータの設定工程を示す説明図である。図の右側に無線通信装置10での処理を示し、左側に無線プリントサーバ20での処理を示した。まず、無線通信装置10側で、無線プリントサーバ20との無線通信を確立するための通信設定を行う（ステップS100）。つまり、無線通信装置10の設定を図1に示した無線プリントサーバ20の設定パラメータに一致させる。但し、この時点で、無線LAN100に接続するための設定パラメータも、無線プリントサーバ20に送信すべき情報として設定パラメータ記憶部14に保持されている。無線プリントサーバ20の設定を行うためのユーティリティソフトによって、この設定パラメータを修正可能としてもよい。

【0034】次に、ユーザによって設定パラメータの送信コマンドが入力されると、簡易暗号通信部13は、既存の設定パラメータを簡易暗号化する（ステップS110）。そして、通信部11は、簡易暗号化された設定デ

ータをバケットに分割し、無線LANカードから無線プリントサーバ20に送信する（ステップS120）。

【0035】無線プリントサーバ20側では、無線通信装置10から送信された簡易暗号化された設定パラメータを通信部21で受信し（ステップS130）、簡易暗号通信部23で簡易復号する（ステップS140）。そして、設定部24が、復号されたデータに基づいてWEPキーを「ABCD」に設定するなど設定パラメータ記憶部25の内容を更新設定する（ステップS150）。以上の工程を経て、無線プリントサーバ20は、無線通信装置10から受信した設定パラメータを用いて既存の無線LAN100に接続することが可能となる。

【0036】以上説明した第1実施例の無線通信装置10および無線プリントサーバ20によれば、設定パラメータを暗号化して無線プリントサーバ20に送信することができるので、設定パラメータの漏洩を回避でき、無線LAN100のセキュリティを確保することができる。

【0037】B. 第2実施例:

B1. 無線通信装置: 図4は、本発明の第2実施例としての無線通信装置10Aおよび無線プリントサーバ20Aの概略構成を示す説明図である。無線通信装置10Aは、第1実施例の無線通信装置10と異なり、簡易暗号通信部13を備えていない。この代わりに、入力部16Aが、無線プリントサーバ20Aとの暗号化通信を確立するためのWEPキーを入力する機能を有している。このWEPキーは、後述する無線プリントサーバ20Aで生成されるものであり、無線LAN100において用いられるWEPキー「ABCD」とは異なる。設定パラメータ記憶部14Aは、既存のWEPキー「ABCD」と新たに入力されるWEPキーとを別々に保持することができる。WEPモジュール12Aは、無線LAN100に接続されているときには、設定パラメータ記憶部14に記憶されている既存のWEPキー「ABCD」を用いて暗号化および復号を行い、無線プリントサーバ20Aと無線通信を行うときには、新たに入力されたWEPキーを用いて暗号化を行う。この他は、第1実施例の無線通信装置10と同じである。

【0038】無線プリントサーバ20Aは、第1実施例の無線プリントサーバ20と異なり、簡易暗号通信部23を備えていない。この代わりに、WEPキー生成部28と、スイッチ29とを備えている。WEPキー生成部28は、ユーザがスイッチ29を操作することによって、WEPキーを乱数的に生成する。ここで、WEPキー生成部28で生成されたWEPキーは、「EFGH」であるものとする。WEPキー「EFGH」は、スプーラ27に送られ、プリンタPRT2の印刷部40によって印刷される。また、WEPキー生成部28は、生成されたWEPキー「EFGH」を設定パラメータ記憶部25に記憶させる。この結果、WEPモジュール22は、

無線通信装置10Aと無線通信を行うときには、WEPキー「EFGH」を用いて通信を行うことが可能となる。この他は、第1実施例の無線プリントサーバ20と同じである。

【0039】B2. パラメータ設定：図5は、第2実施例における設定パラメータの設定工程を示す説明図である。図の右側に無線通信装置10Aでの処理を示し、左側に無線プリントサーバ20Aでの処理を示した。まず、無線プリントサーバ20AのWEPキー生成部28でWEPキーを生成し（ステップS200）、プリンタ

PRT2によって印刷出力する（ステップS210）。これらの工程は、先に説明したように、ユーザがスイッチ29を操作することによって行われる。  
【0040】無線通信装置10A側では、第1実施例と同様に、無線プリントサーバ20Aとの無線通信を確立するための通信設定を行う（ステップS220）。更に、ユーザが無線プリントサーバ20A側で印刷出力されたWEPキー「EFGH」を入力する（ステップS230）。次に、ユーザによって設定パラメータの送信コマンドが入力されると、WEPモジュール12Aは、既存の無線LAN100への接続を確立するための既存の設定パラメータを、入力されたWEPキー「EFGH」を用いて暗号化する（ステップS240）。そして、通信部11は、暗号化された設定パラメータをバケットに分割し、無線LANカードから無線プリントサーバ20Aに送信する（ステップS250）。

【0041】無線プリントサーバ20A側では、無線通信装置10Aから送信された暗号化された設定パラメータを通信部21で受信し（ステップS260）、WEPキー生成部28で生成されたWEPキー「EFGH」を用いて復号する（ステップS270）。そして、設定部24が、復号されたデータに基づいてWEPキーを「ABCD」に変更するなど設定パラメータ記憶部25の内容を更新設定する（ステップS280）。以上の工程を経て、無線プリントサーバ20Aは、無線通信装置10Aから受信した設定パラメータを用いて既存の無線LAN100に接続することが可能となる。

【0042】以上説明した第2実施例の無線通信装置10Aおよび無線プリントサーバ20Aによれば、無線プリントサーバ20Aで乱数的に生成されたWEPキーを用いて設定パラメータを暗号化して無線プリントサーバ20に送信することができるので、設定パラメータの漏洩を回避でき、無線LAN100のセキュリティを確保することができる。

【0043】C. 変形例：以上、本発明のいくつかの実施の形態について説明したが、本発明はこのような実施の形態になんら限定されるものではなく、その要旨を逸脱しない範囲内において種々なる態様での実施が可能である。例えば、以下のような変形例が可能である。

【0044】C1. 変形例1：上記第1実施例では、既

存の設定パラメータの暗号化に単純なスクランブルを用いたが、共通鍵方式による暗号化を用いるものとしてもよい。ここで用いられる共通鍵は、第2実施例と同様の手法により、無線通信装置10側に入力すればよい。

【0045】C2. 変形例2：上記第2実施例では、WEPキー生成部28を備えているが、これを備えないようにしてもよい。この場合、無線プリントサーバ20Aの製造時にデフォルト値として設定パラメータ記憶部25に記憶されたWEPキーを用いるものとしてもよい。デフォルト値として設定されたWEPキーは、第2実施例のように印刷出力してもよいし、装置本体やマニュアル等に記載しておくものとしてもよい。

【0046】C3. 変形例3：上記第2実施例では、WEPキー生成部28で生成されたWEPキーを印刷により出力するものとしたが、これに限られず、ユーザが知ることができるように出力すればよい。従って、例えば、無線プリントサーバ20Aや、プリンタPRT2に表示パネルを設けて表示するようにしてもよいし、音声によって出力するようにしてもよい。

【0047】C4. 変形例4：上記実施例では、本発明を国際標準規格IEEE802.11に基づく無線通信装置に適用した場合について説明したが、これに限られない。本発明は、一般に、一方の無線通信装置から他方の無線通信装置へ、無線通信に用いられる設定パラメータを設定するものであるから、例えば、Bluetooth（商標）やHomeRF（商標）等の規格に基づいた無線通信装置にも適用可能である。この場合、各規格に対応した暗号化技術を適用すればよい。

【0048】C5. 変形例5：上記実施例では、電波を用いた無線暗号通信を例に説明したが、これに限られず、例えば、光や音などを媒体とした無線通信を行う無線通信にも適用可能である。

【図面の簡単な説明】

【図1】無線LAN100の構成を示す説明図である。

【図2】本発明の第1実施例としての無線通信装置10および無線プリントサーバ20の概略構成を示す説明図である。

【図3】第1実施例における設定パラメータの設定工程を示す説明図である。

【図4】本発明の第2実施例としての無線通信装置10Aおよび無線プリントサーバ20Aの概略構成を示す説明図である。

【図5】第2実施例における設定パラメータの設定工程を示す説明図である。

【符号の説明】

10、10A…無線通信装置

11…通信部

12、12A…WEPモジュール

13…簡易暗号通信部

14、14A…設定パラメータ記憶部

11

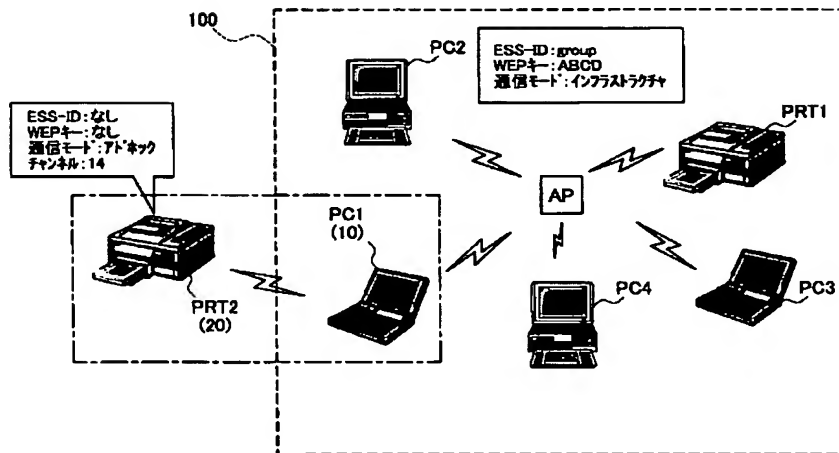
12

15…制御部  
 16、16A…入力部  
 20、20A…無線プリントサーバ  
 21…通信部  
 22…WEPモジュール  
 23…簡易暗号通信部  
 24…設定部

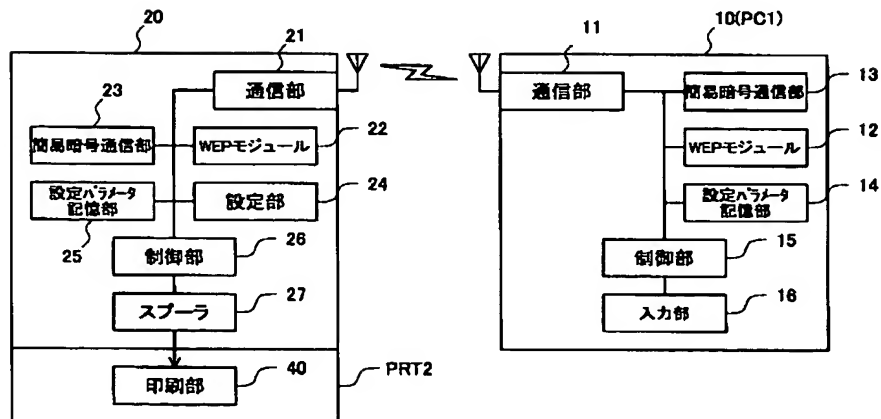
\* 25…設定パラメータ記憶部  
 26…制御部  
 27…スプーラ  
 29…スイッチ  
 40…印刷部  
 100…無線LAN

\*

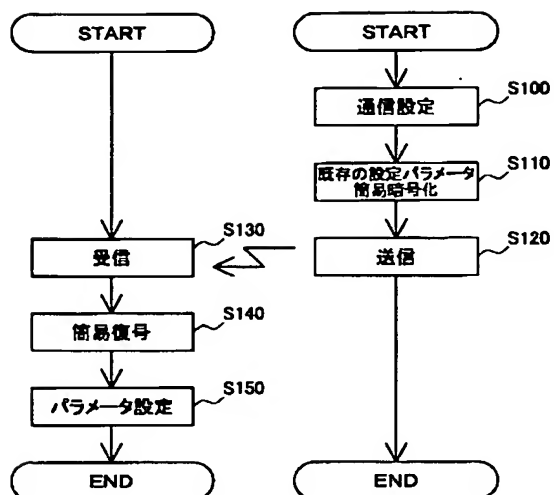
【図1】



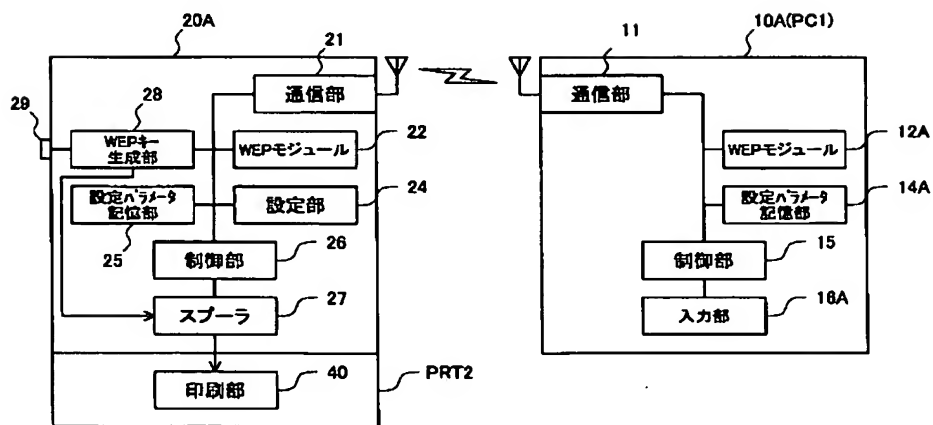
【図2】



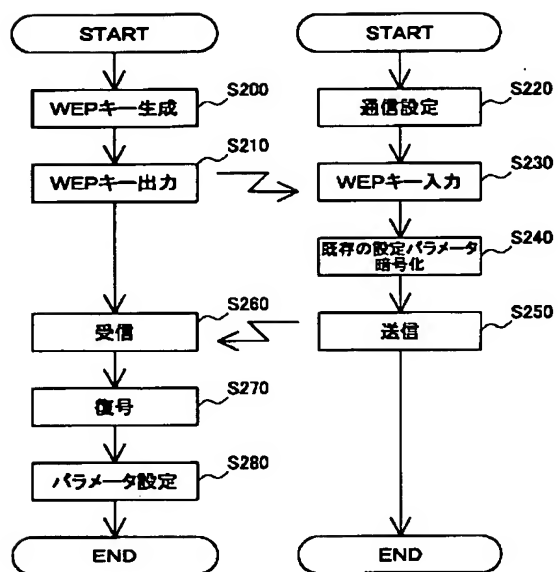
【図3】



【図4】



【図5】



フロントページの続き

Fターム(参考) 5J104 AA01 PA07  
5K033 AA08 DA17  
5K061 AA05 AA09 AA15  
5K067 AA30 BB21 DD17 EE02 EE10  
EE12 HH23 HH36 KK13 KK15